Abstract

This document defines new IPv6 Operations and Management (OAM) capabilities. In order to support these new capabilities, this document defines an IPv6 OAM Option and an ICMPv6 OAM message.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on August 31, 2019.

Copyright Notice

Copyright (c) 2019 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.
1. Problem Statement

This document defines new IPv6 [RFC8200] Operations and Management (OAM) capabilities. In order to support these new capabilities, this document defines an IPv6 OAM Option and an ICMPv6 [RFC4443] OAM message.

2. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. The OAM Option

IPv6 source nodes use the OAM option to invoke one or more OAM actions on downstream devices. The OAM option can be included in any of the following:

- A Hop-by-hop header.

- A Destination Options header that precedes a Routing header.

- A Destination Options header that precedes an upper-layer header.

If a Hop-by-hop header includes an OAM option, OAM actions are invoked on every node along the path to the destination, including the destination (See Note 1). If a Destination Options header that precedes a Routing header includes an OAM option, OAM actions are invoked by the first node that appears in the IPv6 Destination Address field plus subsequent nodes listed in the Routing header. If a Destination Options header that precedes an upper-layer header...
includes an OAM option, OAM actions are invoked on the destination node only.

The OAM option includes the following fields:

- **Option Type (8 bits):** OAM. Value TBD by IANA. See Note 2 and Note 3.
- **Opt Data Len (8 bits):** Length of Option Data, in bytes. Value MUST be equal to 2.
- **Option Data (16 bits):** A bit mask indicating which OAM actions are to be invoked.

<table>
<thead>
<tr>
<th>Bit</th>
<th>Action</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Log the packet</td>
<td>The processing node creates a log entry. The log entry reflects the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>time at which it was created. It also reflects the time at which the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>packet arrived.</td>
</tr>
<tr>
<td>1</td>
<td>Count the packet</td>
<td>The processing node increments a counter.</td>
</tr>
<tr>
<td>2</td>
<td>Send an ICMPv6 OAM</td>
<td>The processing node sends an ICMP OAM message to the packet’s source.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The OAM message indicates the time at which the packet arrived.</td>
</tr>
<tr>
<td>3</td>
<td>Send telemetry</td>
<td>The processing node sends telemetry to a monitoring station.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Telemetry includes the packet and the time at which the packet</td>
</tr>
<tr>
<td></td>
<td></td>
<td>arrived.</td>
</tr>
<tr>
<td>4-15</td>
<td>Reserved</td>
<td></td>
</tr>
</tbody>
</table>

Table 1: Option Data Bits Mapped to OAM Actions

Table 1 maps Option Data bits to OAM actions.

NOTE 1: As per [RFC8200], nodes along a packet’s delivery path only examine and process the Hop-by-Hop Options header if explicitly configured to do so.

NOTE 2: As per [RFC8200], the highest-order two bits of the Option Type (i.e., the "act" bits) specify the action taken by a processing
node that does not recognize Option Type. The required action is skip over this option and continue processing the header. Therefore, IANA is requested to assign this Option Type with "act" bits "00".

NOTE 3: As per [RFC8200], the third-highest-order bit (i.e., the "chg" bit) of the Option Type specifies whether Option Data can change on route to the packet’s destination. Because option data MUST NOT be changed, IANA is requested to assign this Option Type with "chg" bit "0".

3.1. Processing

The processing of OAM actions is optional. If a node does not support particular OAM action, it can ignore the corresponding bit in Option Data.

Having processed an OAM option, the processing node should continue to process the packet. If possible, the OAM action should be executed in parallel with the processing of the rest of the packet.

The processing node SHOULD execute the OAM action, even if it cannot process the packet further. For example, assume the following:

- A node receives a packet.
- The packet contains a Hop-by-hop Options header and the Hop-by-hop Options header includes the OAM option.
- The node does not maintain a route to the packet’s Destination Address

In this case, the node SHOULD execute the requested OAM action. Because the node does not maintain a route to the packet’s Destination Address, it should also send an ICMPv6 Destination Unreachable message to the source node and discard the packet.

4. The ICMPv6 OAM Message
Figure 1 depicts the ICMPv6 OAM message. The ICMPv6 OAM message contains the following fields:

- **Type** - OAM. Value TBD by IANA.
- **Code** - MUST be set to (0) No Error.
- **Checksum** - See [RFC4443]
- **Reserved** - MUST be set to 0 and MUST be ignored upon receipt.
- **Length** - Represents the length of the padded "original datagram" field, measured in 32-bit words.
- **Timestamp (seconds)** - Represents the time at which the original packet arrived in Network Time Protocol (NTP) [RFC5905] format.
- **Timestamp (fraction)** - Represents the time at which the original packet arrived in NTP [RFC5905] format.
- **Original Datagram** - As much of invoking packet as possible without the ICMPv6 packet exceeding the minimum IPv6 MTU (1280 bytes). The original datagram MUST be zero padded to the nearest 32-bit boundary.

ICMPv6 OAM messages SHOULD be rate limited by the sender.

The Timestamp fields SHOULD be as accurate as possible. They SHOULD reflect the time at which the original packet arrived, not the time at which the ICMPv6 OAM message was sent.
5. IANA Considerations

IANA is requested to perform the following actions:

- Allocate a codepoint from the Destination Options and Hop-by-hop Options registry ([https://www.iana.org/assignments/ipv6-parameters/ipv6-parameters.xhtml#ipv6-parameters-2](https://www.iana.org/assignments/ipv6-parameters/ipv6-parameters.xhtml#ipv6-parameters-2)). This option is called "OAM". The "act" bits are 00 and the "chg" bit is 0.

- Create a subregistry in the Destination Options and Hop-by-hop Options registry ([https://www.iana.org/assignments/ipv6-parameters/ipv6-parameters.xhtml#ipv6-parameters-2](https://www.iana.org/assignments/ipv6-parameters/ipv6-parameters.xhtml#ipv6-parameters-2)). This subregistry is called OAM Option Data Bit Mask. Its contents are defined in Table 1 of this document.

- Allocate a codepoint from the "ICMPv6 'type' Numbers" registry ([https://www.iana.org/assignments/icmpv6-parameters/icmpv6-parameters.xml](https://www.iana.org/assignments/icmpv6-parameters/icmpv6-parameters.xml)). This type is called "OAM". As it represents an informational message, its value should be greater than 128.

- Create a "Type x - OAM" subregistry in the "ICMPv6 'type' Numbers" registry ([https://www.iana.org/assignments/icmpv6-parameters/icmpv6-parameters.xml](https://www.iana.org/assignments/icmpv6-parameters/icmpv6-parameters.xml)) registry. This subregistry contains the Code entry (0) No Error.

6. Security Considerations

The following IPv6 extension headers can be used in denial of service attacks:

- The Hop-by-hop header.

- The Destination Options header that precedes a Routing header.

Network operators should block packets containing these extension headers at their boundary.

7. Acknowledgements

The authors acknowledge Ross Callon for his helpful comments.

8. Normative References


Author’s Address

Ron Bonica
Juniper Networks
Herndon, Virginia  20171
USA

Email: rbonica@juniper.net